PATENT ABSTRACTS OF JAPAN

(11) Publication number : 08-249253
(43) Date of publication of application : 27.09.1996

(51) Int. Cl. G06F 13/00
G06F 13/00
G06F 1/00
G09C 1/00
H04L 9/32
H04L 12/00

(21) Application number : 07-052383
(22) Date of filing : 13.03.1995

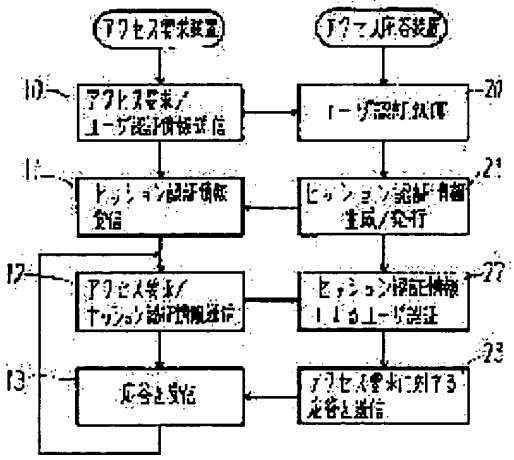
(71) Applicant : FUJITSU LTD
(72) Inventor : MATSUMOTO TATSURO

(54) COMMUNICATION SYSTEM, ACCESS RESPONDER AND ACCESS REQUESTING DEVICE

(57) Abstract:

PURPOSE: To perform the authentication processing of a user on the side of an access requesting device for every access request when access is limited for serive or data held by an access responder.

CONSTITUTION: This access requesting device sends out user authentication information to the access responder only at the time of a first access request relating to a session to be executed (10) and the access responder issues session authentication information valid only for the session of this time at the time of permitting access by the access requesting device by a user authentication processing (21). Thereafter, the access requesting device sends out the session authentication information to the access responder for every access request until the session ends (12) and the access responder uses the session authentication information and performs the user authentication processing (22).



LEGAL STATUS

[Date of request for examination] 02.03.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3463399

[Date of registration] 22.08.2003

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平8－249253

(43)公開日　平成8年(1996)9月27日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	13/00	３５１	7368－5Ｅ	Ｇ０６Ｆ	13/00	３５１Ｚ
		３５７	7368－5Ｅ			３５７Ｚ
	1/00	３７０			1/00	３７０Ｅ
Ｇ０９Ｃ	1/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	Ａ

審査請求　未請求　請求項の数５　ＯＬ　（全 ９ 頁）　最終頁に続く

(21)出願番号　特願平7－52383

(22)出願日　平成７年(1995)３月13日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　松本　達郎
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

(74)代理人　弁理士　井桁　貞一

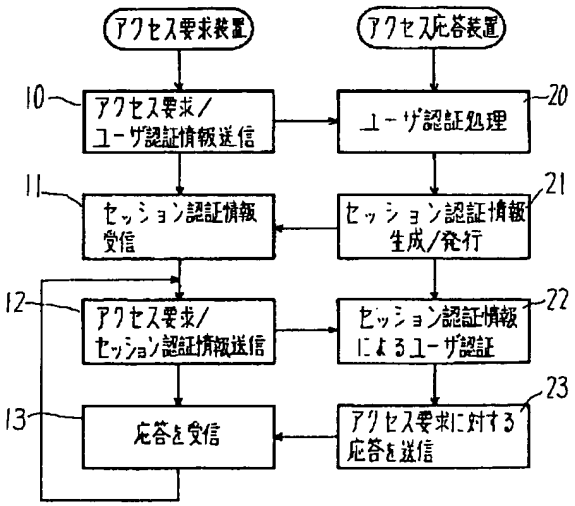
(54)【発明の名称】　通信システムおよびアクセス応答装置およびアクセス要求装置

(57)【要約】　（修正有）

【目的】　アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合、当該アクセス要求の毎にアクセス要求装置側のユーザの認証処理を行う。

【構成】　アクセス要求装置は実行するセッションに係わる最初のアクセス要求時だけアクセス応答装置に対してユーザ認証情報を送出し、アクセス応答装置はユーザ認証処理によりアクセス要求装置によるアクセスを許可した際は、今回のセッションに限り有効なセッション認証情報を発行し、以後アクセス要求装置はセッションが終了するまでに発生するアクセス要求毎にセッション認証情報をアクセス応答装置に送出し、アクセス応答装置は該セッション認証情報を用いてユーザ認証処理を行うように構成する。

本発明の原理説明図



1

【特許請求の範囲】

【請求項1】アクセス要求装置からアクセス応答装置へアクセス要求を行う毎にアクセス要求装置とアクセス応答装置との間のコネクションが確立し，該アクセス要求に対する応答がアクセス応答装置からアクセス要求装置に対してなされた時点でコネクションが解除される通信システムであって、該アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合には、当該アクセス要求の毎にアクセス応答装置側がアクセス要求装置側ユーザの認証処理を行う通信システムにおいて、

前記アクセス要求装置は実行するセッションに係わる最初のアクセス要求時だけ前記アクセス応答装置に対してユーザ認証情報を送出し、前記アクセス応答装置は前記ユーザ認証処理により前記アクセス要求装置によるアクセスを許可した際は、今回のセッションに限り有効なセッション認証情報を発行し、以後前記アクセス要求装置は該セッションが終了するまでに発生するアクセス要求毎に前記セッション認証情報を前記アクセス応答装置に送出し、前記アクセス応答装置は該セッション認証情報を用いてユーザ認証処理を行うように構成したことを特徴とする通信システム。

【請求項2】アクセス要求装置からアクセス応答装置へアクセス要求を行う毎にアクセス要求装置とアクセス応答装置との間のコネクションが確立し，該アクセス要求に対する応答がアクセス応答装置からアクセス要求装置に対してなされた時点でコネクションが解除される通信システムにおけるアクセス応答装置であって、該アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合には、当該アクセス要求毎にアクセス要求装置側ユーザの認証処理を行うアクセス応答装置において、

前記アクセス要求装置からのアクセス要求が該アクセス要求装置が実行するセッションに係わる最初のアクセス要求時であるときは、前記アクセス要求装置から前記ユーザ認証情報を受信して該アクセス要求に対する認証処理を実行し、該アクセス要求を許可した場合は前記セッションに限り有効なセッション認証情報を発行して前記アクセス要求装置に送出し、

以後前記アクセス要求装置から前記セッションに係わるアクセス要求が来たときは、該アクセス要求毎に該アクセス要求装置より前記セッション認証情報を受信して、該セッション認証情報を用いて該アクセス要求に対する認証処理を行うように構成したことを特徴とするアクセス応答装置。

【請求項3】前記セッション期間中のアクセス回数が予め設定された回数を超えた場合は、前記セッション認証情報を無効として前記アクセス要求装置に対して前記ユーザ認証情報の再送信を要求し、前記アクセス要求装置が該要求に応答して送出したユーザ認証情報に基づいてユーザ認証処理を行ったあと、新たなセッション認証情報を前記アクセス要求装置に発行することを特徴とする請求項2に記載のアクセス応答装置。

2

【請求項4】前記セッション期間中のアクセス時間が予め設定された時間を超えた場合は、前記セッション認証情報を無効として前記アクセス要求装置に対して前記ユーザ認証情報の再送信を要求し、前記アクセス要求装置が該要求に応答して送出したユーザ認証情報に基づいてユーザ認証処理を行ったあと、新たなセッション認証情報を前記アクセス要求装置に発行することを特徴とする請求項2に記載のアクセス応答装置。

【請求項5】アクセス要求装置からアクセス応答装置へアクセス要求を行う毎にアクセス要求装置とアクセス応答装置との間のコネクションが確立し，該アクセス要求に対する応答がアクセス応答装置からアクセス要求装置に対してなされた時点でコネクションが解除される通信システムであって、該アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合には、当該アクセス要求の毎にアクセス応答装置側がアクセス要求装置側ユーザの認証処理を行う通信システムにおけるアクセス要求装置において、

実行するセッションに係わる最初のアクセス要求時だけ前記アクセス応答装置に対してユーザ認証情報を送出し、前記アクセス応答装置が前記ユーザ認証処理により前記アクセス要求装置によるアクセスを許可したのに伴い発行したセッション認証情報を受信すると、前記セッションが終了するまでに発生するアクセス要求時には、前記セッション認証情報を前記アクセス応答装置に送出するように構成したことを特徴とするアクセス要求装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はネットワークに接続されたクライアントーサーバシステムなどの通信システムに係わり、特にアクセス要求装置（クライアント等）からアクセス応答装置（サーバ等）へアクセス要求を行う毎にアクセス要求装置とアクセス応答装置との間のコネクションが確立し，該アクセス要求に対する応答がアクセス応答装置からアクセス要求装置に対してなされた時点でコネクションが解除されるシステムであり、かつ該アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合、当該アクセス要求の毎にアクセス要求装置側のユーザの認証処理を行うように構成した通信システム、および該通信システムにて用いられるアクセス応答装置とアクセス要求装置に関する。

【0002】

【従来の技術】近年，コンピュータネットワークの発展は目覚しく，企業／大学内のＬＡＮはもとより，事業所間を結ぶＷＡＮ，また国の基幹となる光ファイバなどを

3

用いた高速なバックボーンネットワークが構築され，さらに世界中の多くの国のネットワーク間が接続されて世界規模の大規模なネットワークが構築されつつある。このように世界中に張り巡らされたコンピュータネットワークを総称してインターネットと呼び，爆発的な勢いで，ネットワークの規模，利用者とも拡大の一途を辿っている。１９９４年現在ではその利用者が世界中で３０００万人に達したと言われている。この急速な利用者の増加をもたらした一因として，WWW(World Wide Web)と呼ばれるシステムの普及が挙げられる。WWWは，HTML(HyperText Markup Language)と呼ばれる記述言語で記述された情報をサーバが保持し，クライアントはURL(Universal Resourece Locator)と呼ばれるリソースの場所（情報のありか）を示す識別子を頼りに，サーバから情報をリトリーブし，ユーザに呈示するものである。WWWでは，これまでのテキスト情報ばかりでなく，サーバ上にある画像や音声の情報に簡単にアクセスできる。そのため，企業や大学のピーアール，オンラインショッピング，電子図書館などに利用され，多くの利用者を集める結果となった。

【０００３】このWWW では、サーバが保持するデータ又はサービスがある特定のユーザだけにしかアクセスできないように制限を設ける必要がある場合は、ユーザＩＤとパスワードを用いて特定ユーザかどうかを認証するように構成している。またWWW ではクライアントからサーバへのアクセス要求が行われる度にコネクションが確立し、アクセス終了時点（先のアクセス要求に対する回答が返ってきた段階）でコネクションが切れるように構成されている。一般的なパソコン通信では一旦回線を接続して端末とセンタとのコネクションが確立した後は、この回線接続を解消する処理を行うまで、端末とホストとのコネクションは継続されるのに対し大きく異なる点である。

【０００４】パソコン通信ではコネクション確立時に認証が実行されるので、コネクションの継続中はアクセス要求毎に認証処理を行う必要はない。しかしWWW ではあるアクセス要求に対する応答がなされる度にクライアント－サーバ間のコネクションが解消されるので、アクセス要求の度にクライアントからサーバに対してＩＤとパスワードとを送出し、認証を行う必要がある。

【０００５】このようなシステムの認証処理を図６を用いてより詳細に説明する。サーバにはクライアントのＩＤとパスワードとの対応関係を登録するテーブルであるＩＤ／パスワードデータベース４と、本来の検索対象であるデータ６とが接続されている。サーバは最初クライアントのアクセス要求待ちの状態にある。この状態の場合、サーバはクライアントからのアクセス要求(80)を受けると、このサーバにはアクセス制限が設けられているので、認証処理を実行するためにＩＤ／パスワード要求(90)をクライアントに対して行なう。

4

【０００６】クライアントでは何らかの手段でＩＤ／パスワードを獲得し（ユーザがその度に入力するか、クライアント側で記憶しておいたＩＤ／パスワードを用いる、等の手段がある）、データ要求と共にＩＤとパスワードをサーバに対して送る(81)。サーバはあらかじめＩＤとパスワードが登録されているＩＤ／パスワードデータベース(4) を検索し，クライアントから送られてきたＩＤ／パスワードの正当性をチェックする(91)。サーバはＩＤ／パスワードが正しければ，サーバが保持しているデータ(6) をクライアントへ送信する(92)。

【０００７】クライアントは，サーバから送られるデータを受け取り，何らかの形（画面表示、音声出力、等）でユーザに当該データを呈示する(82)。さらにデータの要求がある場合，クライアントは(81),(82) の処理，サーバは(91),(92) の処理を繰り返す。

【０００８】

【発明が解決すべき課題】このようにアクセス要求毎にクライアント側からユーザＩＤ／パスワードをサーバへ転送するシステムでは、アクセスの途中でＩＤ／パスワードが盗まれた場合、以後ユーザがＩＤ／パスワードを変更しない限り、ＩＤ／パスワードを盗んだユーザが正当なユーザに代わってデータにアクセスを続けることが可能になる。このため秘密の漏洩が生じることになり、またアクセス毎に課金が課せられるデータの場合，正当なユーザに損害を与えることになる。

【０００９】特に上記のWWW のように、クライアントが実行する１回のセッション（アクセス制限があるデータ／サービスの利用開始から終了までの期間）で複数回のアクセス要求がある場合に、アクセス要求の度にＩＤ／パスワードを送出する必要のあるシステムでは、クライアントが実行する１回のセッション中にも複数回のＩＤ／パスワードの送受信がなされることになるので、ＩＤ／パスワードを盗まれる機会が多く、セキュリティの面で問題がある。

【００１０】本発明はこのような問題点に鑑みなされたものであり、アクセス要求装置（クライアント等）からアクセス応答装置（サーバ等）へアクセス要求を行う毎にアクセス要求装置とアクセス応答装置との間のコネクションが確立し，該アクセス要求に対する応答がアクセス応答装置からアクセス要求装置に対してなされた時点でコネクションが解除されるシステムであり、かつ該アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合、当該アクセス要求の毎にアクセス要求装置側のユーザの認証処理を行うように構成した通信システムにおいて、正当なユーザ認証情報を盗まれる危険性を減少させて、セキュリティを向上させることを目的とする。

【００１１】

【課題を解決するための手段】上記の問題点を解決するために、本発明の通信システムは、アクセス要求装置か

らアクセス応答装置へアクセス要求を行う毎にアクセス要求装置とアクセス応答装置との間のコネクションが確立し，該アクセス要求に対する応答がアクセス応答装置からアクセス要求装置に対してなされた時点でコネクションが解除される通信システムであって、該アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合には、当該アクセス要求の毎にアクセス応答装置側がアクセス要求装置側ユーザの認証処理を行う通信システムにおいて、前記アクセス要求装置は実行するセッションに係わる最初のアクセス要求時だけ前記アクセス応答装置に対してユーザ認証情報を送出し、前記アクセス応答装置は前記ユーザ認証処理により前記アクセス要求装置によるアクセスを許可した際は、今回のセッションに限り有効なセッション認証情報を発行し、以後前記アクセス要求装置は該セッションが終了するまでに発生するアクセス要求毎に前記セッション認証情報を前記アクセス応答装置に送出し、前記アクセス応答装置は該セッション認証情報を用いてユーザ認証処理を行うように構成した。

【００１２】また、アクセス要求装置からアクセス応答装置へアクセス要求を行う毎にアクセス要求装置とアクセス応答装置との間のコネクションが確立し，該アクセス要求に対する応答がアクセス応答装置からアクセス要求装置に対してなされた時点でコネクションが解除される通信システムであって、該アクセス応答装置が保持するデータまたはサービスに対してアクセス制限が課せられたものである場合には、当該アクセス要求毎にアクセス要求装置側ユーザの認証処理を行う通信システムに用いられるアクセス応答装置とアクセス要求装置は、下記のように構成する。

【００１３】アクセス応答装置は、前記アクセス要求装置からのアクセス要求が該アクセス要求装置が実行するセッションに係わる最初のアクセス要求時であるときは、前記アクセス要求装置から前記ユーザ認証情報を受信して該アクセス要求に対する認証処理を実行し、該アクセス要求を許可した場合は前記セッションに限り有効なセッション認証情報を発行して前記アクセス要求装置に送出し、以後前記アクセス要求装置から前記セッションに係わるアクセス要求が来たときは、該アクセス要求毎に該アクセス要求装置より前記セッション認証情報を受信して、該セッション認証情報を用いて該アクセス要求に対する認証処理を行うように構成する。

【００１４】またアクセス要求装置は、実行するセッションに係わる最初のアクセス要求時だけ前記アクセス応答装置に対してユーザ認証情報を送出し、前記アクセス応答装置が前記ユーザ認証処理により前記アクセス要求装置によるアクセスを許可したのに伴い発行したセッション認証情報を受信すると、前記セッションが終了するまでに発生するアクセス要求時には、前記セッション認証情報を前記アクセス応答装置に送出するように構成する。

【００１５】前記のアクセス応答装置は前記セッション期間中のアクセス回数が予め設定された回数を超えた場合、あるいは前記セッション期間中のアクセス時間が予め設定された時間を超えた場合は、前記セッション認証情報を無効として前記アクセス要求装置に対して前記ユーザ認証情報の再送信を要求し、前記アクセス要求装置が該要求に応答して送出したユーザ認証情報に基づいてユーザ認証処理を行ったあと、新たなセッション認証情報を前記アクセス要求装置に発行するように構成しても良い。

【００１６】なお本発明はクライアント－サーバシステムに好適なものであり、この場合はクライアントが前記アクセス要求装置に該当し、サーバが前記アクセス応答装置に該当する。但し本発明はこのクライアント－サーバシステムに限定すべきものではなく、ホスト（センタ）計算機が端末からのアクセス要求を基に処理を行うシステムに導入しても良く、この場合は端末が前記アクセス要求装置に該当し、ホスト計算機が前記アクセス応答装置に該当する。

【００１７】

【作用】本発明は、アクセス要求装置が実行する１回のセッションで複数回のアクセス要求がなされ、このアクセス要求毎にコネクションの確立とアクセス応答装置による認証処理とを行う通信システムに適用される。このような通信システムではユーザ認証情報（例えばアクセス要求装置を利用するユーザ対応に設定されるＩＤと、ＩＤに対応して登録するパスワードとにより構成される）がアクセス要求毎に送受信されることになるので、ユーザ認証情報が盗まれる機会が多い。

【００１８】このため本発明では、図１の原理説明図に示すように、本来の（アクセス要求装置を使用するユーザに固有の）ユーザ認証情報は、アクセス要求装置が実行するセッションに係わり発行する複数のアクセス要求のうち、最初の一回のアクセス要求時のみに送出する(10)。そしてアクセス応答装置では受信したユーザ認証情報に基づいてユーザ認証処理を行い(20)、該ユーザ認証情報が正しい場合は，今回のセッションに限り有効なセッション認証情報を生成して発行し(21)、アクセス要求装置に通知する(11)。この通知を受けたアクセス要求装置は、以後発生するアクセス要求には、このセッション認証情報を付加してアクセス応答装置へ転送する(12)。アクセス応答装置は先に発行してアクセス要求装置に送出したセッション認証情報を用いてユーザ認証を行い(22)、セッション認証情報が正当なものであれば該アクセス要求に対する応答をアクセス要求装置に送出する(23, 13) ように構成した。

【００１９】このように本発明ではアクセス要求装置が実行するセッション中に行われる最初のアクセス要求の時のみ正当なユーザ認証情報を送受信し、その後のアク

セス要求時には実行中のセッションにのみ有効なセッション認証情報を送受信するようにしたので、正当なユーザ認証情報が盗まれる機会を少なくなり、ユーザ認証情報の悪用の危険性が減少する。またセッション認証情報は盗まれたとしても、セッション終了後は無効となるため、他者が悪用することは出来ない。

【００２０】また，予め設定されたアクセス回数またはアクセス時間を超えた場合は、一旦セッション認証情報を無効にした後で新たなセッション認証情報を発行することにより、セッション中にセッション認証情報が盗用されても最小限の被害でくい止めることができる。

【００２１】

【実施例】以下、図面を参照して本発明の実施例を説明する。図２は以下説明する本発明の各実施例が適用されるクライアント―サーバシステムの構成を示すブロック図である。図中、１はクライアント（アクセス要求装置）、２はサーバ（アクセス応答装置）である。複数のクライアント１と複数のサーバが３のネットワークに接続されている。

【００２２】また本実施例においては、クライアント１が各種のデータベースを検索したり、各種のサービスを受けることができるよう、複数のサーバ２が設けられている。例えばサーバ２―１は複数のクライアントがアクセスするデータベースを管理するために設けられたものであり、ＩＤ／パスワードデータベース４とセッションＩＤ／パスワードデータベース５と、クライアントがアクセスする対象である本来のデータが格納されるデータベース６とを有する。

【００２３】ＩＤ／パスワードデータベース４は各ユーザに対応して設けられたＩＤとパスワードとの対応を登録しておくテーブルである。このデータベースには予めクライアントからＩＤとパスワードとを登録する処理が行われ、以後サーバ側ではクライアントから送られるＩＤとパスワードとを用いてユーザ認証処理を行う。セッションＩＤ／パスワードデータベース５は、後で詳述するようにサーバがセッション毎に発行するセッションＩＤとパスワードとを登録するものである。

【００２４】なお本実施例ではＩＤ／パスワードデータベース４とセッションＩＤ／パスワードデータベース５は独立して設けているが、これを纏めて１つのデータベースにして、ユーザＩＤと該ユーザＩＤのクライアントが実行しているセッションに付与されたセッションＩＤ／パスワードとを対応づけるように構成しても良い。更に他のサーバ２―２は通信網７が接続されている。これはパソコン通信に接続して、クライアント１がサーバ２を介してパソコン通信のサービスをも受けられるようにするためのものである。このためサーバ２―２には図示しないが、クライアントから送出されるアクセス要求に基づいてパソコン通信のコマンドを生成し、通信網８に送出する手段と、パソコン通信により得られたデータを当該ネットワーク３で用いられるプロトコルや言語に変換する手段を保有する。なお、このサーバ２―２もサーバ２―１と同様にＩＤ／パスワードデータベースとセッションＩＤ／パスワードデータベースとを有する。

【００２５】このような本実施例でのネットワークシステムでは、クライアント１が例えばサーバ２―１に接続されたデータベース６が有するデータの検索処理を行う場合、検索処理のセッションを実行することになる。但し本システムにおいては検索処理のセッションが継続中であっても、クライアントからサーバへのアクセス要求（検索コマンドの発行）が行われる度にコネクションを確立し、このアクセス要求に対する応答（検索結果の回答）がクライアントに返った段階でコネクションが解消されるようになっている。上記のようにアクセス要求の度にサーバ側でクライアントの認証を行うよう構成されているので、検索処理セッション実行中でも複数回のコネクションの確立と認証処理がなされることになる。

【００２６】またクライアント１がサーバ２―２を用いてパソコン通信を行うセッションを実行する場合は、サーバ２―２はクライアント１からパソコン通信に入る要求を受けた時に通信網７を用いてパソコン通信のホストと接続を行うが、この接続はクライアント１からパソコン通信のセッションが終了する通知を受けるまで継続する。一方クライアント―サーバ間のコネクションは１回のアクセス要求毎に確立し、該アクセス要求に対する応答がなされる度に解消される。またサーバ２―２の認証処理もアクセス要求毎に行われるので、１つのセッションで複数回の認証処理がなされることになる。

【００２７】このようにクライアントが実行する１回のセッションで複数回のアクセス要求がなされ、このアクセス要求毎にコネクションの確立と認証処理を行うシステムでは、ＩＤやパスワードがアクセス要求毎に送受信されることになるので、ＩＤやパスワードが盗まれる危険性が高い。このため本発明では本来のユーザＩＤ／パスワードはセッションの開始時だけ送受信するようにして、セッション中になされるアクセス要求についてはセッション毎に発行されるセッションＩＤ／パスワードを用いて認証処理を行うようにして、本来のユーザＩＤ／パスワードが盗まれる危険性を低くしたことに特徴がある。

【００２８】このようなクライアント―サーバシステムの認証処理について、以下の実施例１～実施例３により更に詳細に説明する。

〔実施例１〕本発明の実施例１の動作を、図３を用いて説明する。この図３では、データベース６を有するサーバ２―１をアクセスする例について説明する。（この説明単に「サーバ」と表記した場合は、サーバ２―１を示す。）

サーバは最初クライアントのアクセス要求の状態にある（200）。この状態からサーバがクライアントからのアク

セス要求(100があると、サーバはＩＤ／パスワード要求(201)をクライアントに対して行なう。

【００２９】クライアントではユーザにＩＤ／パスワードを入力を求め(101)、入力されたＩＤ／パスワードをデータ要求と共にをサーバに対して送る(102)。サーバは予めＩＤ／パスワードが登録されているＩＤ／パスワードデータベース４を検索し，クライアントから送られてきたＩＤ／パスワードの正当性をチェックする(202)。サーバはＩＤ／パスワードが正しければ，乱数を用いてランダムなセッションＩＤ／パスワードを生成し，クライアントへ送信すると共に(210)、生成したセッションＩＤ／パスワードをセッションＩＤ／パスワードデータベース５に登録する。

【００３０】なおセッションＩＤ／パスワードの生成方法としては、上記のような乱数を直接用いる方法の他に、予め複数のセッションＩＤ／パスワードを保持するテーブルを設けておき、発生した乱数で該テーブルを検索し、使用するセッションＩＤ／パスワードを選択する方法も採用し得る。クライアントは受信したセッションＩＤ／パスワードを記憶する(110)。以後クライアントは現在実行中のセッションが終了するまで、該セッションに係わるアクセス要求には、下記の通り全てセッションＩＤ／パスワードを付与する。

【００３１】クライアントがデータ要求を行なうと(120)、サーバはセッションＩＤ／パスワードを要求する(220)。クライアントはセッションＩＤ／パスワードをサーバに対して送信する(121)。サーバはセッションＩＤ／パスワードデータベース５を検索して、送られてきたセッションＩＤ／パスワードが正しいかどうかチェックする(221)。セッションＩＤ／パスワードが正しい場合，サーバが保持しているデータ６をクライアントへ送信する(230)。クライアントはサーバから送られるデータを受信し、画面表示や音声出力等を用いてユーザに当該データを呈示する(132)。

【００３２】さらに実行中のセッションの終了までに、該セッションに関してデータの要求がある場合、クライアントは上記(120)～(132)の処理，サーバは(220)～(230)の処理を繰り返す。即ちクライアントは先にサーバが発行したセッションＩＤ／パスワードをデータ要求の度に送出し、サーバはこのセッションＩＤ／パスワードを用いて認証処理を行う。

【００３３】ユーザがセッションを終る場合は，データ表示終了後，ユーザがセッション終了の入力を起こすと(140)，サーバに対してセッション終了通知が行なわれる(141)。サーバはセッション終了通知を受け取ると(240)，セッションＩＤ／パスワードデータベース中の今回のセッションＩＤ／パスワードをクリアし(241)，最初のアクセス要求待ち(200)の状態に戻る。

【００３４】また先述したサーバによるセッションＩＤ／パスワードのチェック(221)にてセッションＩＤ／パスワードが正しくない場合は，サーバはクライアントに対してエラーを通知し(223)、データ要求待ちの状態(240)となる。クライアントは受信したデータがエラーを示すものである場合は，サーバから再びデータ要求(120)を行うか、セッション終了の通知(141)を行う。

【００３５】〔実施例２〕図４を用いて本発明の実施例２を説明する。本実施例２も上記の実施例１と同様に図２の構成にてクライアント１－１がサーバ２－１をアクセスする例を説明するものである。　図４で図３と同一の処理については図３と同一の参照符号を付与している。このように本実施例の処理動作は基本的に実施例１と同様のものであるので、後述する相違点以外の処理については実施例１の説明を参照されたい。

【００３６】本実施例と実施例１との相違点は、実施例１ではクライアント側でセッションを終了させるまで、当該セッションについては同一のセッションＩＤ／パスワードを用いるのに対し、本実施例ではサーバはクライアントから送出されるアクセス回数が一定回数を超えた場合には、サーバは一旦使用中のセッションＩＤ／パスワードを無効にして、新たなセッションＩＤ／パスワードを発行するようにしたことにある。

【００３７】この処理を図４を用いて説明する。サーバが以前なされたアクセス要求に対する応答のデータ送信をクライアントに対して実行した(230)後で、アクセス回数が予め設定された回数に達したか否かを判定し、該アクセス回数が所定の回数を越えた場合は(250)、今回のセッションＩＤ／パスワードをクリア(241)して，再びアクセス要求待ちの状態(200)にする。ユーザが再びデータへアクセスする場合は，本来のＩＤ／パスワードの入力を行ない，セッションＩＤ／パスワードを取得しなければならない。

【００３８】本実施例によると，アクセス回数が所定回数を越えた時点で，これまでのセッションＩＤ／パスワードを無効にし，新しいセッションＩＤ／パスワードを生成するため，セッションＩＤ／パスワードがセッション中に盗用されても最小限の被害で食い止めることができる。

〔実施例３〕図５を用いて本発明の実施例３を説明する。本実施例３も上記の実施例１，２と同様に図２の構成にてクライアント１－１がサーバ２－１をアクセスする例を説明するものである。

【００３９】図５で図３と同一の処理については図３と同一の参照符号を付与している。このように本実施例の処理動作は基本的に実施例１と同様のものであるので、後述する相違点以外の処理については実施例１の説明を参照されたい。本実施例と実施例１との相違点は、実施例１ではクライアント側でセッションを終了させるまで、当該セッションについては同一のセッションＩＤ／パスワードを用いるのに対し、本実施例ではサーバはクライアントとのアクセス時間を監視して、アクセス時間

11

が予め定められた一定時間を超えた場合には、サーバは一旦使用中のセッションＩＤ／パスワードを無効にして、新たなセッションＩＤ／パスワードを発行するようにしたことにある。

【００４０】この処理を図５を用いて説明する。サーバはクライアントから最初にアクセス要求があった時間からの経過時間を測定し、このアクセス時間が所定の時間を越えた場合(260)、今回のセッションＩＤ／パスワードをクリア(241)して，再びアクセス要求待ちの状態(200)とする。ユーザが再びデータへアクセスする場合は，本来のＩＤ／パスワードの入力を行ない，セッションＩＤ／パスワードを取得しなければならない。

【００４１】本実施例によると，アクセス時間が所定時間を越えた時点で，これまでのセッションＩＤ／パスワードを無効にし，新しいセッションＩＤ／パスワードを生成するため，セッションＩＤ／パスワードがセッション中に盗用されても最小限の被害で食い止めることができる。

【００４２】

【効果】以上説明したように、本発明の通信システムによれば、アクセス要求装置が実行するセッションに係わる複数のアクセス要求をアクセス応答装置に送出する場合に、最初のアクセス要求だけ本来のユーザ認証情報を

12

送ってユーザ認証処理を行うようにし、以降はセッションに対応して生成されるセッション認証情報を用いてサーバ上のデータにアクセスするために，本来のＩＤ／パスワードを盗用される確率が低くなり，セッションＩＤ／パスワードが盗まれた場合でもセッション終了後は無効となるため，サーバ上のデータのセキュリティが強化される。

【図面の簡単な説明】

【図１】本発明の原理説明図である。

【図２】本発明のクライアントーサーバシステムの一例を示す構成ブロック図である。

【図３】本発明の実施例１の動作を説明する図である。

【図４】本発明の実施例２の動作を説明する図である。

【図５】本発明の実施例３の動作を説明する図である。

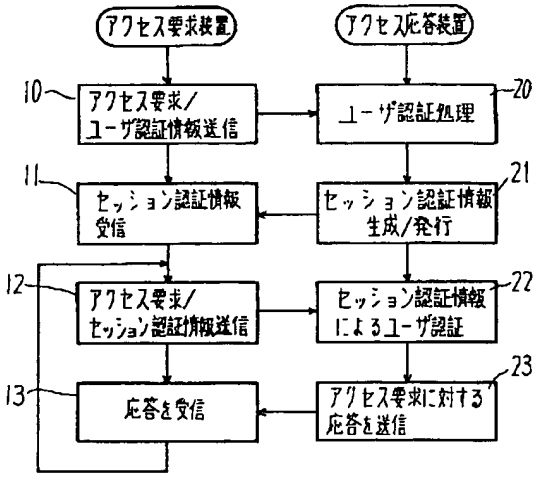
【図６】従来技術の説明図である。

【符号の説明】

1　クライアント
2　サーバ
3　ネットワーク
4　ＩＤ／パスワードデータベース
5　セッションＩＤ／パスワードデータベース
6　データベース
7　通信網

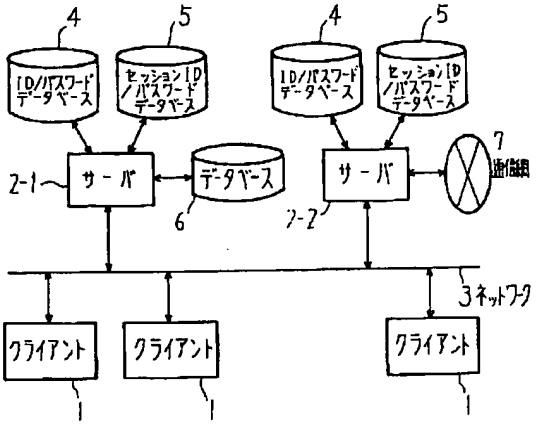
【図１】

本発明の原理説明図



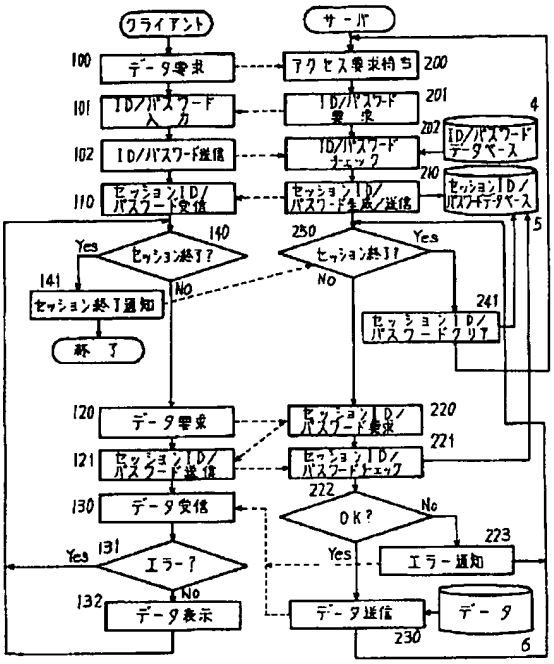
【図２】

クライアントーサーバシステムの構成の一例を示す図



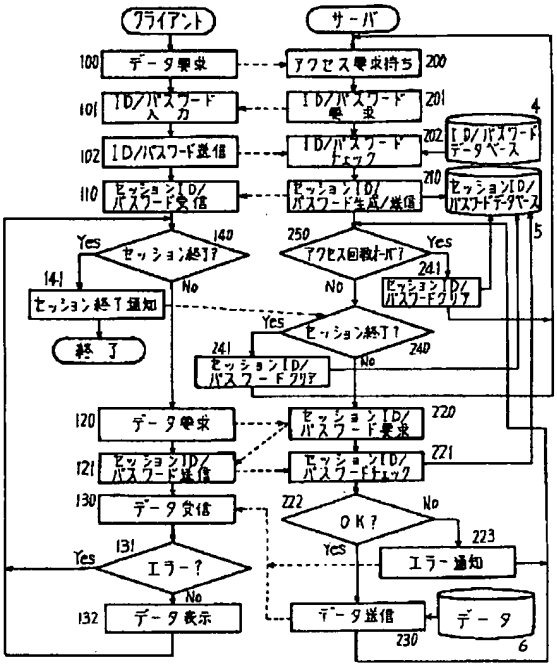
【図3】

本発明の実施例1



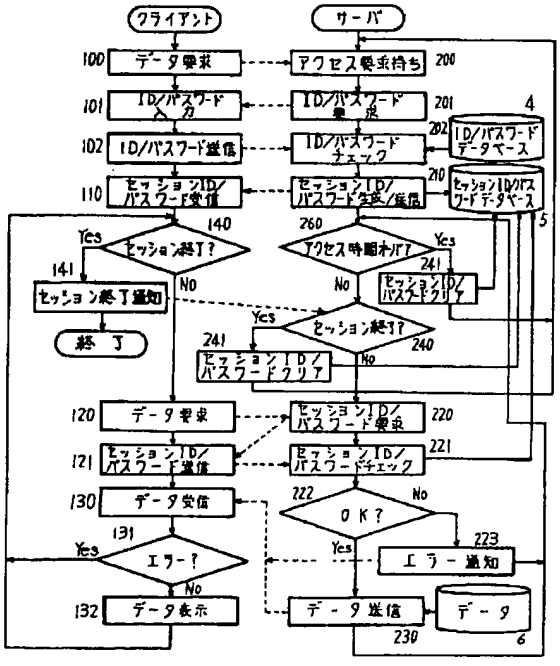
【図4】

本発明の実施例2



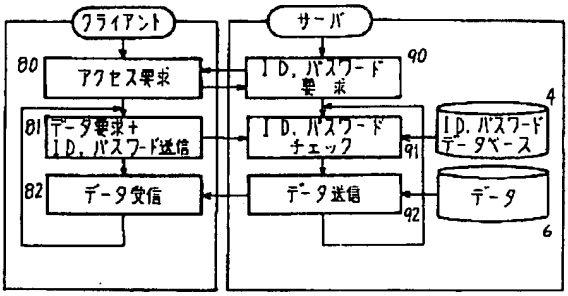
【図5】

本発明の実施例3



【図6】

従来方式



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　12/00		9466－5K	Ｈ０４Ｌ　11/00	